Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

020.201 Server Patch Management

Version 2.2
December 15, 2017

Revision History

Date	Version	Description	Author
9/2/2002	1.0	Effective Date	CHFS IT Policies Team Charter
12/15/2017	2.2	Revision Date	CHFS OATS Policy Charter Team
12/15/2017	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	12/15/2017	ROBERT E PUTT	
CHFS Chief Information Security Officer (or designee)	12/15/2017	DENNIS E. LEBER	

Table of Contents

020.201 Server Patch Management Policy

Category: 020.200 Managerial Security

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a server patch management policy. This document establishes the agency's Server Patch Management Policy which helps manage patching cycles and provides guidelines for security best practices regarding patch management.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) for exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restricted access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 *Roles and Responsibilities*

2.1 Chief Information Security Officer (CISO)

This positon is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of this policy along with the OATS Information Security (IS) Team.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer positon is an attorney within CHFS Office of Legal Services (OLS). This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position will be responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notification in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contract Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3 Policy Requirements

3.1 General Server Patch Management

Hardware and operating system patches will be applied monthly by COT to CHFS servers, per their patch cycle. Emergency patches will be applied to all CHFS servers as soon as possible.

3.2 Patch Cycle Stages

COT will apply patches in four (4) stages:

- Stage 1- Patches will be applied to all Development environment servers.
- Stage 2- Patches will be applied to all Test environment servers.
- Stage 3- Patches will be applied to all UAT and Training environment servers.
- Stage 4- Patches will be applied to all Production environment servers.

COT will work with the agency for any downtime that may be required.

3.3 Emergency and Out of Band Patches

COT will apply emergency and out of band patches per approval from the Office of the Secretary IT Executive, Chief Information Security Officer (CISO), and the OATS IS Team.

Service Packs and/or Releases are considered upgrades to the Operating System and will be handled on a case by case basis.

4 Policy Definitions

- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Emergency/Out of Band Patches:** Microsoft released patches released at some time other than the normal release window and the patch’s deployment into production is scheduled on an approved date/time agreed upon between COT and the agency(s).
- **In-Scope Servers:** any server connected to a CHFS network managed by COT must follow the guidelines outlined above.
- **Production*:*** any server not in the Development, Test, or User Acceptance Testing/Training (UAT) environments. All servers are labeled (Development, Test, Production, etc.) in Information Technology Management Portal (ITMP). For example, File Servers are labeled as Production.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data.

Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS IT Policies
- CHFS OATS IT Standards
- CHFS OATS Policy: 010.103- Change Control Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Policy: CIO-082- Critical Systems Vulnerability Assessment Policy
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-12 An Introduction to Computer Security
- National Institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information